Available online at www.sciencedirect.com
ScienceDirect
Journal of Symbolic Computation 43 (2008) 293–303
Journal of Symbolic Computation
www.elsevier.com/locate/jsc

Descent via isogeny on elliptic curves with large rational torsion subgroups

E.V. Flynn [1], C. Grattoni

Mathematical Institute, University of Oxford, 24–29 St. Giles', Oxford OX1 3LB, United Kingdom

Received 7 December 2006; accepted 6 November 2007
Available online 12 November 2007

Abstract

We outline PARI programs which assist with various algorithms related to descent via isogeny on elliptic curves. We describe, in this context, variations of standard inequalities which aid the computation of members of the Tate–Shafarevich group. We apply these techniques to several examples: in one case we use descent via 9-isogeny to determine the rank of an elliptic curve; in another case we find nontrivial members of the 9-part of the Tate–Shafarevich group, and in a further case, nontrivial members of the 13-part of the Tate–Shafarevich group.

Keywords: Elliptic curves; Isogeny; Tate–Shafarevich group

1. Introduction

We shall consider the technique of descent via d-isogeny for computing the rank of an elliptic curve $\mathcal{E}$, defined over $\mathbb{Q}$, which has a $\mathbb{Q}$-rational point of prime power order d. As we shall mention later, these techniques can be extended to any curve that admits a rational isogeny; however, we restrict ourselves to elliptic curves with a $\mathbb{Q}$-rational torsion point for the sake of computational convenience. The descent technique that we make explicit in this article can be done over a quotient group of the rational numbers when a curve has a nontrivial rational torsion point, while computations for curves with no rational torsion points, but admitting a rational isogeny, must be done over a (sometimes large degree) number field. By a theorem of Mazur (see

E-mail addresses: flynn@maths.ox.ac.uk (E.V. Flynn), grattoni@gmail.com (C. Grattoni).
[1] Tel.: +44 1865 289076; fax: +44 1865 273583.

0747-7171/$ - see front matter
doi:10.1016/j.jsc.2007.11.001

Mazur (1978), Theorem 4.1) we know that $d \in \{2, 3, 4, 5, 7, 8, 9\}$. Specific numerical examples of descent via d-isogeny for the cases $d \in \{2, 3, 4, 5, 7, 8\}$ can be found, for example, in Beaver (2000), Cassels (1959), Cremona et al. (2006), Cremona and Serf (1999), Delong (2002), Elkies and Rogers (2004), Fisher (2000, 2001), Goins (2004), Merriman et al. (1996), Schaefer and Stoll (2004), Silverman (1986), Stamminger (2005) and Top (1993). In addition, mwrank (Cremona, 2005) can be used to perform a full 2-descent and Magma (2007) can be used to perform various descents, including descent via 3-isogeny. Our main purpose here is to describe our programs in PARI (Batut et al., 2007) which assist with descent via isogeny in this context. These include implementations of the method of Vélu (1971) for describing the isogenous curve $\widehat{\mathcal{E}}$, for which there are d-isogenies $\phi : \mathcal{E} \to \widehat{\mathcal{E}}$ and $\widehat{\phi} : \widehat{\mathcal{E}} \to \mathcal{E}$, the method described by Schaefer (1998) for constructing injections on $\mathcal{E}(\mathbb{Q})/\widehat{\phi}(\widehat{\mathcal{E}}(\mathbb{Q}))$ and $\widehat{\mathcal{E}}(\mathbb{Q})/\phi(\mathcal{E}(\mathbb{Q}))$ into quotient groups of extensions of $\mathbb{Q}$ modulo dth powers, and various programs for performing local techniques in the search for independent points in $\mathcal{E}(\mathbb{Q}_p)/\widehat{\phi}\big(\widehat{\mathcal{E}}(\mathbb{Q}_p)\big)$, so that overall the Selmer bound on the rank can be computed. These programs will help others to compute isogeny-Selmer bounds more easily. We demonstrate these programs with examples of descent via 9-isogeny, in one case computing the rank, and in another case proving the existence of a member of the 9-part of the Tate–Shafarevich group. We shall also derive an inequality (which follows from combining special cases of several standard results) which allows members of the Tate–Shafarevich group to be found, while bypassing much of the hard work of the d-Selmer group computations. We apply this to the case $d = 13$ (where there can be a $\mathbb{Q}$-rational subgroup of order 13 even though there is no $\mathbb{Q}$-rational point of order 13) to derive a member of the 13-part of the Tate–Shafarevich group. Specifically we shall show, as Example 3 in Section 5, that the elliptic curve

$$\widehat{\mathcal{E}} : y^2 + xy + y = x^3 - x^2 - 911\,138\,880x - 10\,586\,098\,442\,003$$

is such that $\#Ш(\widehat{\mathcal{E}}/\mathbb{Q})[13] \geq 13^2$.

We have given in Flynn and Grattoni (2007) all of the PARI programs, and a more detailed description of the following techniques.

2. Isogenies

We first recall the fact (see Husemöller (2003), 4.1) that any elliptic curve, defined over $\mathbb{Q}$, with a $\mathbb{Q}$-rational point P, not of order 1, 2, 3, can be birationally transformed to the *Tate normal form*:

$$y^2 + (1 - w)xy + vy = x^3 + vx^2, \text{ where } v, w \in \mathbb{Q}, \tag{1}$$

where the identity is $\mathcal{O}$, the point at infinity, and P has been mapped to $(0, 0)$. If we now compute $d(0, 0) = \big(f(v, w)/h(v, w), g(v, w)/h(v, w)\big)$, where $f(v, w), g(v, w), h(v, w) \in \mathbb{Q}[v, w]$, then $h(v, w) = 0$ gives an equation sufficient for $(0, 0)$ to be d-torsion. When $d \in \{2, 3, 4, 5, 6, 7, 8, 9, 10, 12\}$ the curve defined by $h(v, w) = 0$ is of genus 0 (see Conrad and Rubin (2001)) and can be parametrized, giving

$$\mathcal{E}_t^d : y^2 + j_d(t)xy + k_d(t)y = x^3 + k_d(t)x^2, \quad t \in \mathbb{Q},\ \Delta(\mathcal{E}_t^d) \neq 0, \tag{2}$$

where $j_d(t), k_d(t)$ are rational functions in t. For example, $(0, 0)$ is a point of order 9 on

$$\begin{aligned}\mathcal{E}_t^9 : {} & y^2 + (t^3 + t^2 + 1)xy + t^2(t^3 + 2t^2 + 2t + 1)y \\ & = x^3 + t^2(t^3 + 2t^2 + 2t + 1)x^2,\ t \in \mathbb{Q},\ t \neq 0, -1.\end{aligned} \tag{3}$$

We now recall the method described by Vélu (1971) for constructing isogenies between elliptic curves with a nontrivial torsion subgroup defined over $\mathbb{Q}$. Let

$$\mathcal{E} : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{4}$$

be an elliptic curve with a point $T \in \mathcal{E}(\overline{\mathbb{Q}})$ of order d, such that $\langle T\rangle$, the subgroup generated by T, is defined over $\mathbb{Q}$. For any $P_0 = (x_0, y_0)$ let $x(P_0), y(P_0)$ denote x_0, y_0, respectively. The intuitive idea behind Vélu's technique is to define $X(P), Y(P)$ which are invariant under $P \mapsto P + P'$, for any $P' \in \langle T\rangle$. We therefore take sums over all members of $\langle T\rangle$, in defining the functions

$$\begin{aligned} X(P) &= x(P) + \sum_{Q\in\langle T\rangle-\{\mathcal{O}\}} \Big(x(P+Q) - x(Q)\Big),\\ Y(P) &= y(P) + \sum_{Q\in\langle T\rangle-\{\mathcal{O}\}} \Big(y(P+Q) - y(Q)\Big). \end{aligned} \tag{5}$$

The map $P \mapsto (X(P), Y(P))$ will be our required isogeny, and it remains to find the curve satisfied by $X(P), Y(P)$. We associate the following values to the elliptic curve given in (4):

$$b_2 = a_1^2 + 4a_2, \quad b_4 = 2a_4 + a_1a_3, \quad b_6 = a_3^2 + 4a_6. \tag{6}$$

Let $\langle T\rangle_2$ denote the points of order 2 in $\langle T\rangle$. Further, let R be a subset of $\langle T\rangle - \{\mathcal{O}\} - \langle T\rangle_2$ such that $\langle T\rangle - \{\mathcal{O}\} - \langle T\rangle_2 = R \cup (-R)$ and $R \cap (-R) = \varnothing$. Let $S = R \cup \langle T\rangle_2$, and define the following quantities for any $Q \in \mathcal{E}(\mathbb{Q})$:

$$\begin{aligned} &g_Q^x = 3x(Q)^2 + 2a_2x(Q) + a_4 - a_1y(Q), \quad g_Q^y = -2y(Q) - a_1x(Q) - a_3,\\ &u_Q = (g_Q^y)^2 = 4x_Q^3 + b_2x_Q^2 + 2b_4x_Q + b_6,\\ &s_Q = \begin{cases} g_Q^x & \text{if } Q \in \langle T\rangle_2\\ 2g_Q^x - a_1g_Q^y = 6x_Q^2 + b_2x_Q + b_4 & \text{if } Q \notin \langle T\rangle_2, \end{cases}\\ &s = \sum_{Q\in S} s_Q, \quad w = \sum_{Q\in S}(u_Q + x_Qt_Q). \end{aligned}$$

Theorem 1 (*Vélu*). *Let $\mathcal{E}$ be as in (4), with T a point of order d, and s, w be the above quantities. Then $\phi : P \mapsto \big(X(P), Y(P)\big)$ of (5) is an isogeny with kernel $\mathcal{E}(\mathbb{C})[\phi] = \langle T\rangle$ from $\mathcal{E}$ to the elliptic curve*

$$\widehat{\mathcal{E}} : Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + (a_4 - 5s)X + (a_6 - b_2s - 7w). \tag{7}$$

Proof. See Vélu (1971), where this relation between X and Y is obtained via the formal groups of $\mathcal{E}$ and $\widehat{\mathcal{E}}$. □

Applying Vélu's method to $\mathcal{E}_t^d$ gives an isogeny ϕ to

$$\widehat{\mathcal{E}}_t^d : Y^2 + j_d(t)XY + k_d(t)Y = X^3 + k_d(t)X^2 + l_d(t)X + m_d(t). \tag{8}$$

For example, as before, $j_9(t) = (t^3 + t^2 + 1)$, $k_9(t) = t^2(t^3 + 2t^2 + 2t + 1)$ and

$$\begin{aligned} l_9(t) &= 5t(t^{10} + t^9 - 8t^8 - 33t^7 - 72t^6 - 108t^5 - 114t^4 - 81t^3 - 37t^2 - 10t - 1),\\ m_9(t) &= t^{17} - 7t^{16} - 63t^{15} - 230t^{14} - 641t^{13} - 1639t^{12} - 3691t^{11} - 6707t^{10} - 9425t^9\\ &\quad - 10\,174t^8 - 8456t^7 - 5379t^6 - 2559t^5 - 865t^4 - 190t^3 - 24t^2 - t. \end{aligned} \tag{9}$$

Further, we can apply Vélu's method to $\widehat{\mathcal{E}}_t^d$ (after first factoring the dth division polynomial of $\widehat{\mathcal{E}}_t^d$ to compute the kernel) to find an isogeny to $\widehat{\widehat{\mathcal{E}}}_t^d$, the dual curve to $\widehat{\mathcal{E}}_t^d$, which is birationally equivalent to $\mathcal{E}_t^d$. This yields the dual isogeny, $\hat{\phi} : \widehat{\mathcal{E}}_t^d \to \mathcal{E}_t^d$.

We have made available in Flynn and Grattoni (2007) tables of $j_d(t), k_d(t), l_d(t), m_d(t)$, as well as the short PARI (Batut et al., 2007) functions `TorsionCurve`, `DualCurve`, `IsogenyPhi` and `IsogenyDual`, which find $\mathcal{E}_t^d, \widehat{\mathcal{E}}_t^d, \phi, \hat{\phi}$.

3. The $\widehat{\phi}$-Selmer and Tate–Shafarevich groups

Let $\widehat{\phi} : \widehat{\mathcal{E}} \to \mathcal{E}$ be a $\mathbb{Q}$-rational isogeny of elliptic curves defined over $\mathbb{Q}$, let $G = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, $G_p = \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$, and define the $\widehat{\phi}$-Selmer group $\mathrm{Sel}^{(\widehat{\phi})}(\widehat{\mathcal{E}}/\mathbb{Q})$ and the Tate–Shafarevich group $Ш(\widehat{\mathcal{E}}/\mathbb{Q})$ by

$$\mathrm{Sel}^{(\widehat{\phi})}(\widehat{\mathcal{E}}/\mathbb{Q}) = \ker\left(H^1(G, \widehat{\mathcal{E}}(\overline{\mathbb{Q}})[\widehat{\phi}]) \to \prod_p H^1(G_p, \widehat{\mathcal{E}}(\overline{\mathbb{Q}}_p)) \right) \tag{10}$$

and

$$Ш(\widehat{\mathcal{E}}/\mathbb{Q}) = \ker\left(H^1(G, \widehat{\mathcal{E}}(\overline{\mathbb{Q}})) \to \prod_p H^1(G_p, \widehat{\mathcal{E}}(\overline{\mathbb{Q}}_p)) \right). \tag{11}$$

For future reference, we fix the notation $\Delta_{\min}(\mathcal{E})$ to denote the discriminant of a minimal model for $\mathcal{E}$, let $\mathcal{E}_0(\mathbb{Q}_p)$ denote the set of points in $\mathcal{E}(\mathbb{Q}_p)$ which are nonsingular after reduction modulo p, let $c_{\mathcal{E},p} = \#\mathcal{E}(\mathbb{Q}_p)/\mathcal{E}_0(\mathbb{Q}_p)$ be the Tamagawa number for $\mathcal{E}$ at p, and similarly let $c_{\widehat{\mathcal{E}},p}$ be the Tamagawa number for $\widehat{\mathcal{E}}$ at p. Furthermore, let

$$\begin{aligned} S = \{p : p | \Delta_{\min}(\mathcal{E}) \text{ or } p | d \text{ or } p = \infty\} - \{p : \ \gcd(d, c_{\mathcal{E},p}) = \ \gcd(d, c_{\widehat{\mathcal{E}},p}) = 1\}, \\ \mathbb{Q}(S, d) = \{k \in \mathbb{Q}^*/(\mathbb{Q}^*)^d : \mathrm{ord}_p(k) \equiv 0 \bmod d \text{ for all } p \notin S\}. \end{aligned} \tag{12}$$

We recall the following standard result, which uses an explicit description of the Weil pairing in this context.

Theorem 2 (*Silverman, 1986, X.1.1 and Exercise 10.1*). *Let $\mathcal{E}$ be an elliptic curve defined over $\mathbb{Q}$ and let $\phi : \mathcal{E} \to \widehat{\mathcal{E}}$ be a degree-d $\mathbb{Q}$-rational isogeny such that $\mathcal{E}(\mathbb{C})[\phi]$ is generated by a point $T \in \mathcal{E}(\mathbb{Q})$ of order d. Then there exists $f_T \in \mathbb{Q}(\mathcal{E})$ such that $div(f_T) = d \cdot T - d \cdot \mathcal{O}$ and $f_T \circ \widehat{\phi} = g_T^d$ for some $g_T \in \mathbb{Q}(\widehat{\mathcal{E}})$. Furthermore, the map $F : \mathcal{E}(\mathbb{Q})/\widehat{\phi}(\widehat{\mathcal{E}}(\mathbb{Q})) \to \mathbb{Q}^*/(\mathbb{Q}^*)^d$, $P \mapsto f_T(P)$ is an injective homomorphism, satisfying $imF \leqslant \mathbb{Q}(S, d)$.*

It is worth briefly mentioning here what happens in the more general context when $\mathcal{E}(\mathbb{C})[\phi]$ is defined over $\mathbb{Q}$, even though there is no $\mathbb{Q}$-rational point T of order d. The simplest case of this is a curve of the form $\mathcal{E} : y^2 = x^3 + k$, where $k \in \mathbb{Q}^*$ but $k \notin (\mathbb{Q}^*)^2$, when there is a 3-isogeny ϕ, defined over $\mathbb{Q}$, from $\mathcal{E}$ to the curve $\widehat{\mathcal{E}} : y^2 = x^3 - 27k$. This situation is described, for example, on p. 65 of Cassels (1995). In this case $\mathcal{E}(\mathbb{C})[\phi] = \{\mathcal{O}, (0, \sqrt{k}), (0, -\sqrt{k})\}$, and the generalisation of the above map gives instead a map $F : \mathcal{E}(\mathbb{Q})/\widehat{\phi}(\widehat{\mathcal{E}}(\mathbb{Q})) \to K^*/(K^*)^3$, where $K = \mathbb{Q}(\sqrt{k})$, the field of definition of a generator $(0, \sqrt{k})$ of $\mathcal{E}(\mathbb{C})[\phi]$. In the general case, when ϕ has order d, and $\mathcal{E}(\mathbb{C})[\phi]$ is defined over $\mathbb{Q}$, even though there is no $\mathbb{Q}$-rational point T of order d, the degree of the number field K will typically increase with d, and be bounded above by $d - 1$. We shall not require this level of generality in our examples, as they will always have an actual $\mathbb{Q}$-rational point T of order d.

For example, if $\mathcal{E}_t^9, \widehat{\mathcal{E}}_t^9$ are the 9-isogenous curves in (3), (8) and (9), then $F^9(P)$, for any $P = (x, y)$, is:

$$\begin{aligned} F^9(x,y) \;=\; & (-t^2-2)x^4 + (-2t^4 - t^3 - 2t^2 + (y-1))x^3 + (-t^6 - 2t^5 - 3t^4 - 2t^3 \\ & + (3y-1)t^2 + 3y)x^2 + (3yt^4 + 2yt^3 + 3yt^2 + y)x \\ & + (yt^6 + 2yt^5 + 3yt^4 + 2yt^3 + yt^2). \end{aligned} \tag{13}$$

We let

$$F_p : \mathcal{E}(\mathbb{Q}_p)/\widehat{\phi}(\widehat{\mathcal{E}}(\mathbb{Q}_p)) \to \mathbb{Q}_p^*/(\mathbb{Q}_p^*)^d,\ P \mapsto f_T(P) \tag{14}$$

be defined in an analogous manner to F where p can be any prime, including the prime at infinity. We also define $\beta_p : \mathbb{Q}(S,d) \to \mathbb{Q}_p^*/(\mathbb{Q}_p^*)^d$ as the map induced by the natural embedding $\mathbb{Q}^* \to \mathbb{Q}_p^*$. Then

$$\begin{aligned} \mathcal{E}(\mathbb{Q})/\widehat{\phi}(\widehat{\mathcal{E}}(\mathbb{Q})) \;\cong\; \mathrm{im}F \leqslant \mathrm{Sel}^{(\widehat{\phi})}(\widehat{\mathcal{E}}/\mathbb{Q}) \cong \bigcap_{p\in S} \beta_p^{-1}\Big(F_p\Big(\mathcal{E}(\mathbb{Q}_p)/\widehat{\phi}\big(\widehat{\mathcal{E}}(\mathbb{Q}_p)\big)\Big)\Big) \\ \leqslant \mathbb{Q}(S,d) \leqslant \mathbb{Q}^*/(\mathbb{Q}^*)^d. \end{aligned} \tag{15}$$

Let $\mathcal{E}, \widehat{\mathcal{E}}$ be the isogenous elliptic curves of (4) and (7), with $\phi((x,y)) = (X,Y)$, and let $z = -x/y$ and $Z = -X/Y$ be the respective local parameters around $\mathcal{O}$, the point at infinity. (see Silverman (1986), IV.1.1.2). Then Z can be written as a power series $Z = f(z) \in \mathbb{Q}[[z]]$, and we define define γ_ϕ to be norm of the leading coefficient of $f(z)$. Similarly, we can write $z = F(Z) \in \mathbb{Q}[[Z]]$, and define $\gamma_{\widehat{\phi}}$. to be the norm of the leading coefficient of $F(Z)$. Note that for our $\mathcal{E}_t^d, \widehat{\mathcal{E}}_t^d$ of (2) and (8), we always have $\gamma_\phi = 1$ and $\gamma_{\widehat{\phi}} = d$.

Lemma 1 (*Schaefer, 1996, 3.8*). *Let $\mathcal{E}$ be an elliptic curve defined over $\mathbb{Q}$ and let $\phi : \mathcal{E} \to \widehat{\mathcal{E}}$ be a degree-d $\mathbb{Q}$-rational isogeny where d is a power of a prime and $\mathcal{E}(\mathbb{C})[\phi]$ is generated by a point $T \in E(\mathbb{Q})$. Let p be a finite prime. Then*

$$\#\mathcal{E}(\mathbb{Q}_p)/\widehat{\phi}(\widehat{\mathcal{E}}(\mathbb{Q}_p)) = |\gamma_{\widehat{\phi}}|_p^{-1} \#\widehat{\mathcal{E}}(\mathbb{Q}_p)[\widehat{\phi}]\, \frac{c_{\mathcal{E},p}}{c_{\widehat{\mathcal{E}},p}}. \tag{16}$$

Further, when $p = \infty$, if $d = 2^k$, $k \geqslant 1$, then $\#\mathcal{E}(\mathbb{R})/\widehat{\phi}(\widehat{\mathcal{E}}(\mathbb{R})) = 1$ or 2; otherwise, $\#\mathcal{E}(\mathbb{R})/\widehat{\phi}(\widehat{\mathcal{E}}(\mathbb{R})) = 1$.

For finite p, we can apply Hensel's Lemma together with searches modulo a suitable power of p, until the number of computed distinct members of $\mathcal{E}(\mathbb{Q}_p)/\widehat{\phi}(\widehat{\mathcal{E}}(\mathbb{Q}_p))$ equals the right-hand side of (16). At $p = \infty$, we have $\mathbb{Q}_p = \mathbb{R}$ and the question of whether $\#\mathcal{E}(\mathbb{R})/\widehat{\phi}(\widehat{\mathcal{E}}(\mathbb{R})) = 1$ or 2 is easy to resolve, as it is equivalent to deciding whether there exists $P = (x,y) \in \mathcal{E}(\mathbb{R})$ such that $F_\infty(P) < 0$. If $(x, y_1(x))$, $(x, y_2(x))$ denote the two points with the same x-coordinate, then this is merely a matter of examining the range of $F_\infty(x, y_1(x))$ and $F_\infty(x, y_2(x))$, for $x \in \mathbb{R}$. In all cases, it is straightforward to compute $\mathcal{E}(\mathbb{Q}_p)/\widehat{\phi}(\widehat{\mathcal{E}}(\mathbb{Q}_p))$. One can then compute $\mathrm{Sel}^{(\widehat{\phi})}(\widehat{\mathcal{E}}/\mathbb{Q})$ by computing $\bigcap_{p\in S} \beta_p^{-1}\big(F_p\big(\mathcal{E}(\mathbb{Q}_p)/\widehat{\phi}\big(\widehat{\mathcal{E}}(\mathbb{Q}_p)\big)\big)\big)$ and applying (15). When this has the same order as do the known members of $\mathcal{E}(\mathbb{Q})/\widehat{\phi}(\widehat{\mathcal{E}}(\mathbb{Q}))$, then the latter is also computed. When there is a nontrivial member of $Ш(\widehat{\mathcal{E}}/\mathbb{Q})[\widehat{\phi}]$, then this method will not determine $\mathcal{E}(\mathbb{Q})/\widehat{\phi}(\widehat{\mathcal{E}}(\mathbb{Q}))$.

The `IsPrincipal` function in Magma (2007) applied to $d \cdot T - d \cdot \mathcal{O}$ (which computes f_T such that $\mathrm{div}(f_T) = d \cdot T - d \cdot \mathcal{O}$), can be used to find the map F in Theorem 2. We have applied this to the $\mathcal{E}_t^d(\mathbb{Q})$ of (2) to create, and place in Flynn and Grattoni (2007), a table of the resulting

map F in these cases, which we have also included in our PARI function Fo. We have also placed in Flynn and Grattoni (2007) our PARI functions `ModuloPowLocalp`, which computes $\beta_p(z)$, `FpSearchp`, which performs a naive search for the members of $\mathcal{E}(\mathbb{Q}_p)/\widehat{\phi}(\widehat{\mathcal{E}}(\mathbb{Q}_p))$. Note also that the Tamagawa numbers $c_{\mathcal{E},p}$,$c_{\widehat{\mathcal{E}},p}$ can be easily computed using functions built into Magma (2007) or PARI (Batut et al., 2007). A general algorithm for computing Tamagawa numbers for elliptic curves can be found in Tate (1975). Finally, determining $\#\widehat{\mathcal{E}}(\mathbb{Q}_p)[\widehat{\phi}]$ is a direct application of Hensel's Lemma.

4. Ratio theorems and $Ш(\mathcal{E}/\mathbb{Q})[d]$

We first recall the standard observation that we can compute the rank r of $\mathcal{E}(\mathbb{Q})$ by finding $\mathcal{E}(\mathbb{Q})/[d]\mathcal{E}(\mathbb{Q})$ for some integer $d > 1$, since $\mathcal{E}(\mathbb{Q}) \cong \mathcal{E}_{\text{tors}}(\mathbb{Q}) \times \mathbb{Z}^r$ implies $\mathcal{E}(\mathbb{Q})/[d]\mathcal{E}(\mathbb{Q}) \cong \mathcal{E}_{\text{tors}}(\mathbb{Q})/[d]\mathcal{E}_{\text{tors}}(\mathbb{Q}) \times (\mathbb{Z}/2\mathbb{Z})^r$ and $\mathcal{E}_{\text{tors}}(\mathbb{Q})/[d]\mathcal{E}_{\text{tors}}(\mathbb{Q})$ is straightforward to compute. The previous section has described how to compute $\text{Sel}^{(\widehat{\phi})}(\widehat{\mathcal{E}}/\mathbb{Q})$, which sometimes allows the computation of $\mathcal{E}(\mathbb{Q})/\widehat{\phi}(\widehat{\mathcal{E}}(\mathbb{Q}))$. Furthermore, when $[d] = \hat{\phi}\phi$, we have the following lemma.

Lemma 2 (*See Schaefer and Stoll (2004)*). *Let $\phi : \mathcal{E} \to \widehat{\mathcal{E}}$ be degree-d $\mathbb{Q}$-rational isogeny, with $[d] = \hat{\phi}\phi$. Then the sequence*

$$\begin{aligned} 0 \to \widehat{\mathcal{E}}(\mathbb{Q})[\widehat{\phi}]/\phi(\mathcal{E}(\mathbb{Q})[d]) \to Sel^{(\phi)}(\mathcal{E}/\mathbb{Q}) \to Sel^{(d)}(\mathcal{E}/\mathbb{Q}) \\ \to Sel^{(\widehat{\phi})}(\widehat{\mathcal{E}}/\mathbb{Q}) \to Ш(\widehat{\mathcal{E}}/\mathbb{Q})[\widehat{\phi}]/\phi(Ш(\mathcal{E}/\mathbb{Q})[d]) \to 0 \end{aligned} \tag{17}$$

and its subsequence

$$\begin{aligned} 0 \to \widehat{\mathcal{E}}(\mathbb{Q})[\widehat{\phi}]/\phi(\mathcal{E}(\mathbb{Q})[d]) \to \widehat{\mathcal{E}}(\mathbb{Q})/\phi(\mathcal{E}(\mathbb{Q})) \xrightarrow{\hat{\phi}} \mathcal{E}(\mathbb{Q})/[d]\mathcal{E}(\mathbb{Q}) \\ \to \mathcal{E}(\mathbb{Q})/\widehat{\phi}(\widehat{\mathcal{E}}(\mathbb{Q})) \to 0 \end{aligned} \tag{18}$$

are both exact.

From this, it is apparent that $\text{Sel}^{(d)}(\mathcal{E}/\mathbb{Q})$ (and therefore the rank of $\mathcal{E}(\mathbb{Q})$ if there are no nontrivial members of $Ш(\mathcal{E}/\mathbb{Q})[d]$) can be deduced from $\text{Sel}^{\phi}(\mathcal{E}/\mathbb{Q})$ and $\text{Sel}^{(\widehat{\phi})}(\widehat{\mathcal{E}}/\mathbb{Q})$, each of which can be computed as in the previous section. However, it can happen that one of these is much easier to compute, in which case the following result (used in Schaefer and Stoll (2004) to perform descent via isogeny) is helpful.

Theorem 3 (*Cassels, 1965*). *Let $\mathcal{E}$ be as in (4) and $\phi : \mathcal{E} \to \widehat{\mathcal{E}}$ be as in Lemma 2. Then*

$$\frac{\#Sel^{(\phi)}(\mathcal{E}/\mathbb{Q})}{\#Sel^{(\widehat{\phi})}(\widehat{\mathcal{E}}/\mathbb{Q})} = \frac{\#\mathcal{E}(\mathbb{Q})[\phi]\ \ \Omega_{\widehat{\mathcal{E}}}\ \ \prod_p c_{\widehat{\mathcal{E}},p}}{\#\widehat{\mathcal{E}}(\mathbb{Q})[\widehat{\phi}]\ \ \Omega_{\mathcal{E}}\ \ \prod_p c_{\mathcal{E},p}}, \quad \text{where } \Omega_{\mathcal{E}} = \int_{\mathcal{E}(\mathbb{R})} \left| \frac{\mathrm{d}x}{2y + a_1x + a_3} \right|. \tag{19}$$

The quantities $\Omega_{\mathcal{E}}$, $\Omega_{\widehat{\mathcal{E}}}$ (as with $c_{\mathcal{E},p}, c_{\widehat{\mathcal{E}},p}$) can be easily computed using functions built into Magma (2007) or PARI (Batut et al., 2007). Now we see that Cassels' ratio theorem gives us a method for trying to compute $\mathcal{E}(\mathbb{Q})/[d]\mathcal{E}(\mathbb{Q})$ (and thus the rank of $\mathcal{E}(\mathbb{Q})$) simply by finding $\text{Sel}^{(\widehat{\phi})}(\widehat{\mathcal{E}}/\mathbb{Q})$. Explicitly, we can combine Theorem 3 and (18) from Lemma 2 to obtain

$$\begin{aligned} \#\text{Sel}^{(d)}(\mathcal{E}/\mathbb{Q}) &\leqslant \frac{\#\text{Sel}^{(\phi)}(\mathcal{E}/\mathbb{Q}) \cdot \#\text{Sel}^{(\widehat{\phi})}(\widehat{\mathcal{E}}/\mathbb{Q})}{\#\widehat{\mathcal{E}}(\mathbb{Q})[\widehat{\phi}]/\phi(\mathcal{E}(\mathbb{Q})[d])} \\ &= \frac{\#\mathcal{E}(\mathbb{Q})[\phi]\ \ \Omega_{\widehat{\mathcal{E}}}\ \ \prod_p c_{\widehat{\mathcal{E}},p}}{\#\widehat{\mathcal{E}}(\mathbb{Q})[\widehat{\phi}]\ \ \Omega_{\mathcal{E}}\ \ \prod_p c_{\mathcal{E},p}} \cdot \frac{\#\text{Sel}^{(\widehat{\phi})}(\widehat{\mathcal{E}}/\mathbb{Q})}{\#\widehat{\mathcal{E}}(\mathbb{Q})[\widehat{\phi}]/\phi(\mathcal{E}(\mathbb{Q})[d])}. \end{aligned}$$

In addition, as long as $Ш(\widehat{\mathcal{E}}/\mathbb{Q})[\widehat{\phi}]/\phi(Ш(\mathcal{E}/\mathbb{Q})[d])$ is trivial, this will be an equality. Now the standard exact sequence (see Silverman (1986), X.4.2.a)

$$0 \to \mathcal{E}(\mathbb{Q})/[d]\mathcal{E}(\mathbb{Q}) \to \mathrm{Sel}^{(d)}(\mathcal{E}/\mathbb{Q}) \to Ш(\mathcal{E}/\mathbb{Q})[d] \to 0 \tag{20}$$

gives that $\#\mathcal{E}(\mathbb{Q})/[d]\mathcal{E}(\mathbb{Q}) \leqslant \#\mathrm{Sel}^{(d)}(\mathcal{E}/\mathbb{Q})$ and so, in summary,

$$\begin{aligned} \#\mathcal{E}(\mathbb{Q})/[d]\mathcal{E}(\mathbb{Q}) &\leqslant \#\mathrm{Sel}^{(d)}(\mathcal{E}/\mathbb{Q}) \\ &\leqslant \frac{\#\mathcal{E}(\mathbb{Q})[\phi]\ \ \Omega_{\widehat{\mathcal{E}}}\ \ \prod_p c_{\widehat{\mathcal{E}},p}}{\#\widehat{\mathcal{E}}(\mathbb{Q})[\widehat{\phi}]\ \ \Omega_{\mathcal{E}}\ \ \prod_p c_{\mathcal{E},p}} \cdot \frac{\#\mathrm{Sel}^{(\widehat{\phi})}(\widehat{\mathcal{E}}/\mathbb{Q})}{\#\widehat{\mathcal{E}}(\mathbb{Q})[\widehat{\phi}]/\phi(\mathcal{E}(\mathbb{Q})[d])}, \end{aligned} \tag{21}$$

where everything becomes an equality when $Ш(\widehat{\mathcal{E}}/\mathbb{Q})[\widehat{\phi}]/\phi(Ш(\mathcal{E}/\mathbb{Q})[d])$ and $Ш(\mathcal{E}/\mathbb{Q})[d]$ are trivial. We now outline the descent process we have used; see Djabri et al. (2000), Schaefer (1998), Schaefer and Stoll (2004) for examples using a similar approach.

Input: $d \in \{4, 5, 7, 8, 9\}$ and $t \in \mathbb{Q}$ corresponding to the elliptic curve $\mathcal{E} = \mathcal{E}_t^d$ of (2).

Output: $\frac{\#\mathrm{Sel}^{(\phi)}(\mathcal{E}/\mathbb{Q})\cdot\#\mathrm{Sel}^{(\widehat{\phi})}(\widehat{\mathcal{E}}/\mathbb{Q})}{\#\widehat{\mathcal{E}}(\mathbb{Q})[\widehat{\phi}]/\phi(\mathcal{E}(\mathbb{Q})[d])}$, which serves as an upper bound for $\#\mathcal{E}(\mathbb{Q})/[d]\mathcal{E}(\mathbb{Q})$.

Step 1: Compute $\mathrm{Sel}^{(\widehat{\phi})}(\widehat{\mathcal{E}}/\mathbb{Q})$ using (15), by finding $\bigcap_{p\in S} \beta_p^{-1}\big(F_p\big(\mathcal{E}(\mathbb{Q}_p)/\widehat{\phi}\big(\widehat{\mathcal{E}}(\mathbb{Q}_p)\big)\big)\big)$.

Step 2: Use Theorem 3 to compute the size of $\mathrm{Sel}^{(\phi)}(\mathcal{E}/\mathbb{Q})$.

Step 3: Use the inequality in (21), to find upper bounds for $\#\mathrm{Sel}^{(d)}(\mathcal{E}/\mathbb{Q})$ $\#\mathcal{E}(\mathbb{Q})/[d]\mathcal{E}(\mathbb{Q})$.

Recall that as long as $Ш(\widehat{\mathcal{E}}/\mathbb{Q})[\widehat{\phi}]/\phi(Ш(\mathcal{E}/\mathbb{Q})[d])$ and $Ш(\mathcal{E}/\mathbb{Q})[d]$ are both trivial, then our upper bound on $\#\mathcal{E}(\mathbb{Q})/[d]\mathcal{E}(\mathbb{Q})$ is actually an equality. We can then perform a naïve search on $\mathcal{E}(\mathbb{Q})$ to try to determine whether our bound is attained. We can use, for example, the PARI function of Womack (2000) which uses height pairing matrices to determine when points are independent. If we find enough points to verify that the above bound is an equality, we terminate the algorithm and return the rank of $\mathcal{E}(\mathbb{Q})$.

Remark 1. We have made available at Flynn and Grattoni (2007) the PARI function `SelmerBound(d, t)`. For example:

`SelmerBound(5, 4)` returns 5, giving that the rank of $\mathcal{E}_4^5 : y^2 + 5xy + 4y = x^3 + 4x^2$ is 0 and $\mathcal{E}_4^5(\mathbb{Q}) \cong \mathbb{Z}/5\mathbb{Z}$.

While we will use Theorem 3 theorem mainly for the purpose of finding the order of $\mathrm{Sel}^{(\phi)}(\mathcal{E}/\mathbb{Q})$ from the order of $\mathrm{Sel}^{(\widehat{\phi})}(\widehat{\mathcal{E}}/\mathbb{Q})$, we show that a variation allows $Ш(\mathcal{E}/\mathbb{Q})[d]$ to be proved nontrivial, without performing the hard work of a descent via ϕ-isogeny. Kloosterman and Schaefer (2003), Kloosterman (2005), and Matsuno (2007) have used Theorem 3 to obtain similar results.

Proposition 1. *Let $\phi : \mathcal{E} \to \widehat{\mathcal{E}}$ be as in Lemma 2. Then*

$$\begin{aligned} \#Ш(\mathcal{E}/\mathbb{Q})[d] \geqslant &\left(\frac{\#\mathcal{E}(\mathbb{Q})[\phi]\ \ \Omega_{\widehat{\mathcal{E}}}\ \ \prod_p c_{\widehat{\mathcal{E}},p}}{\#\widehat{\mathcal{E}}(\mathbb{Q})[\widehat{\phi}]\ \ \Omega_{\mathcal{E}}\ \ \prod_p c_{\mathcal{E},p}}\right)\left(\frac{1}{\#\widehat{\mathcal{E}}(\mathbb{Q})[\widehat{\phi}]/\phi(\mathcal{E}(\mathbb{Q})[d])}\right) \\ &\times \left(\frac{1}{\#\mathcal{E}(\mathbb{Q})/[d]\mathcal{E}(\mathbb{Q})}\right). \end{aligned}$$

Proof. Combining Theorem 3 and (17) from Lemma 2 gives

$$\#\mathrm{Sel}^{(d)}(\mathcal{E}/\mathbb{Q}) \geqslant \frac{\#\mathrm{Sel}^{(\phi)}(\mathcal{E}/\mathbb{Q})}{\#\widehat{\mathcal{E}}(\mathbb{Q})[\widehat{\phi}]/\phi(\mathcal{E}(\mathbb{Q})[d])} \geqslant \left(\frac{\#\mathrm{Sel}^{(\phi)}(\mathcal{E}/\mathbb{Q})}{\#\mathrm{Sel}^{(\widehat{\phi})}(\widehat{\mathcal{E}}/\mathbb{Q})}\right)\left(\frac{1}{\#\widehat{\mathcal{E}}(\mathbb{Q})[\widehat{\phi}]/\phi(\mathcal{E}(\mathbb{Q})[d])}\right)$$
$$= \left(\frac{\#\mathcal{E}(\mathbb{Q})[\phi]\ \ \Omega_{\widehat{\mathcal{E}}}\ \ \prod_p c_{\widehat{\mathcal{E}},p}}{\#\widehat{\mathcal{E}}(\mathbb{Q})[\widehat{\phi}]\ \ \Omega_{\mathcal{E}}\ \ \prod_p c_{\mathcal{E},p}}\right)\left(\frac{1}{\#\widehat{\mathcal{E}}(\mathbb{Q})[\widehat{\phi}]/\phi(\mathcal{E}(\mathbb{Q})[d])}\right).$$

Furthermore, sequence (20) gives $\#\mathrm{Sel}^{(d)}(\mathcal{E}/\mathbb{Q}) = \#\mathcal{E}(\mathbb{Q})/[d]\mathcal{E}(\mathbb{Q}) \cdot \#Ш(\mathcal{E}/\mathbb{Q})[d]$ which, when combined with the above inequality, gives the required result. □

Suppose now that $\phi : \mathcal{E} \to \widehat{\mathcal{E}}$ is a degree-d $\mathbb{Q}$-rational isogeny of $\mathbb{Q}$-rational elliptic curves, and suppose that $Ш(\mathcal{E}/\mathbb{Q})[2]$ is trivial so that a complete 2-descent on $\mathcal{E}$ yields that the rank of $\mathcal{E}(\mathbb{Q})$ is some $r \in \mathbb{Z}^+$. By also computing $\mathcal{E}_{\mathrm{tors}}(\mathbb{Q})$, we can immediately find $\#\mathcal{E}(\mathbb{Q})/[d]\mathcal{E}(\mathbb{Q}) \subseteq \mathrm{Sel}^{(d)}(\mathcal{E}/\mathbb{Q})$. It is similarly an easy task to compute the other quantities on the right-hand side of Proposition 1. If this exceeds 1, then we have verified that $Ш(\mathcal{E}/\mathbb{Q})[d]$ is nontrivial, without having actually performed a descent via ϕ-isogeny.

5. Worked-out examples

We shall give several examples to illustrate the above ideas, emphasising descent via 9-isogeny and 13-isogeny. We shall give here only the main steps of each example, and have placed the details in Flynn and Grattoni (2007).

Example 1. The elliptic curve

$$\mathcal{E} : y^2 + 13xy + 84y = x^3 + 84x^2$$

has $\mathrm{rank}(\mathcal{E}(\mathbb{Q})) = 1$.

Proof. We show this by performing a 9-descent on $\mathcal{E}$. Let $d = 9$ and $t = 2$, so that our curves $\mathcal{E}_t^d$ and $\widehat{\mathcal{E}}_t^d$ of (3), (8) and (9) are:

$$\mathcal{E} : y^2 + 13xy + 84y = x^3 + 84x^2 \quad \text{and}$$
$$\widehat{\mathcal{E}} : y^2 + 13xy + 84y = x^3 + 84x^2 - 154\,410 - 41\,506\,050.$$

Further, $S = \{2, 3, 7, 37\}$. Our injection (13) then becomes

$$F : \mathcal{E}(\mathbb{Q})/\widehat{\phi}(\widehat{\mathcal{E}}(\mathbb{Q})) \to \mathbb{Q}(S, 9),$$
$$(x, y) \mapsto -6x^4 + (y - 49)x^3 + (15y - 196)x^2 + 77yx + 196y.$$

Now, we can apply Lemma 1 to obtain:

$$\beta_2^{-1}\left(F_2\left(\mathcal{E}(\mathbb{Q}_2)/\widehat{\phi}\left(\widehat{\mathcal{E}}(\mathbb{Q}_2)\right)\right)\right) = \langle 2, 3, 7, 37\rangle,$$
$$\beta_7^{-1}\left(F_7\left(\mathcal{E}(\mathbb{Q}_7)/\widehat{\phi}\left(\widehat{\mathcal{E}}(\mathbb{Q}_7)\right)\right)\right) = \langle 2^1 \cdot 3^1, 2^3 \cdot 7^3, 3^3 \cdot 7^3\rangle,$$
$$\beta_3^{-1}\left(F_3\left(\mathcal{E}(\mathbb{Q}_3)/\widehat{\phi}\left(\widehat{\mathcal{E}}(\mathbb{Q}_3)\right)\right)\right) = \langle 2, 3, 7, 37\rangle,$$
$$\beta_{37}^{-1}\left(F_{37}\left(\mathcal{E}(\mathbb{Q}_{37})/\widehat{\phi}\left(\widehat{\mathcal{E}}(\mathbb{Q}_{37})\right)\right)\right) = \langle 2^1 \cdot 3^1, 3^5 \cdot 7^1\rangle,$$

with no further information provided at infinity. We apply (15) and take the intersection of these, obtaining

$$\begin{aligned}\mathrm{Sel}^{(\widehat{\phi})}(\widehat{\mathcal{E}}/\mathbb{Q}) &= \langle 2^1\cdot 3^1, 2^3\cdot 7^3, 3^3\cdot 7^3\rangle \bigcap \langle 2^1\cdot 3^1, 3^5\cdot 7^1\rangle \bigcap \langle 2,3,7,37\rangle \\ &= \langle 2^1\cdot 3^1, 2^3\cdot 7^3\rangle \cong \mathbb{Z}/9\mathbb{Z}\times\mathbb{Z}/3\mathbb{Z},\end{aligned}$$

so that $\#\mathrm{Sel}^{(\widehat{\phi})}(\widehat{\mathcal{E}}/\mathbb{Q}) = 27$. Using the formula from Theorem 3, we see that this implies $\#\mathrm{Sel}^{(\phi)}(\mathcal{E}/\mathbb{Q}) = 3$. Since also $\#\widehat{\mathcal{E}}(\mathbb{Q})[\widehat{\phi}] = 1$, the exact sequence (17) from Lemma 2, gives:

$$\#\mathrm{Sel}^{(9)}(\mathcal{E}/\mathbb{Q}) \leqslant \frac{\#\mathrm{Sel}^{(\widehat{\phi})}(\widehat{\mathcal{E}}/\mathbb{Q})\cdot\#\mathrm{Sel}^{(\phi)}(\mathcal{E}/\mathbb{Q})}{\#\mathcal{E}(\mathbb{Q})[\phi]} = 9^2,$$

so that $\#\mathcal{E}(\mathbb{Q})/[9]\mathcal{E}(\mathbb{Q}) \leqslant 9^2$. A short search on $\mathcal{E}(\mathbb{Q})$ yields the point $(-21/4, 315/8)$ of infinite order. Since also $\#\mathcal{E}_{\mathrm{tors}}(\mathbb{Q})/9\mathcal{E}_{\mathrm{tors}}(\mathbb{Q}) = \#\mathcal{E}_{\mathrm{tors}}(\mathbb{Q}) = 9$, it follows that $\#\mathcal{E}(\mathbb{Q})/[9]\mathcal{E}(\mathbb{Q}) = 9^2$, and that $\mathcal{E}(\mathbb{Q})$ has rank 1. We have therefore computed the rank using only computations in $\mathbb{Q}$ and various $\mathbb{Q}_p$, whereas a 2-descent would have required computations over a cubic number field. □

Example 2. The elliptic curve

$$\mathcal{E}: y^2 + \frac{11}{8}xy + \frac{21}{32}y = x^3 + \frac{21}{32}x^2$$

has $\mathrm{rank}(\mathcal{E}(\mathbb{Q})) = 1$. Further,

$$\widehat{\mathcal{E}}: y^2 + \frac{11}{8}xy + \frac{21}{32}y = x^3 + \frac{21}{32}x^2 - \frac{190\,905}{2048}x - \frac{49\,989\,225}{131\,072}$$

is such that $Ш(\widehat{\mathcal{E}}/\mathbb{Q})[3^\infty] \cong \mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/3\mathbb{Z}$.

Proof. Let $d = 9$ and $t = 1/2$, so that our curves $\mathcal{E}_t^d$ and $\widehat{\mathcal{E}}_t^d$ of (3), (8) and (9) are:

$$\begin{aligned}&\mathcal{E}: y^2 + \frac{11}{8}xy + \frac{21}{32}y = x^3 + \frac{21}{32}x^2 \quad \text{and} \\ &\widehat{\mathcal{E}}: y^2 + \frac{11}{8}xy + \frac{21}{32}y = x^3 + \frac{21}{32}x^2 - \frac{190\,905}{2048}x - \frac{49\,989\,225}{131\,072}.\end{aligned}$$

Applying Proposition 1, with $\mathcal{E}, \widehat{\mathcal{E}}$ interchanged, and computing all of the values for c, Ω, and $E(\mathbb{Q})/[d]E(\mathbb{Q})$ (from $E(\mathbb{Q})/[2]E(\mathbb{Q})$) in Magma, gives:

$$\#Ш(\widehat{\mathcal{E}}/\mathbb{Q})[9] \geqslant \left(\frac{1\cdot(9\Omega_{\widehat{\mathcal{E}}})\cdot 243}{9\cdot(\Omega_{\widehat{\mathcal{E}}})\cdot 3}\right)\left(\frac{1}{9}\right)\left(\frac{1}{1}\right) = 9. \tag{22}$$

Note that the above global Tamagawa number of 243 for $\mathcal{E}$ in the numerator, was obtained as the product of the Tamagawa numbers at $2, 3, 7$, which were $9, 9, 3$, respectively. The global Tamagawa number of 3 for $\widehat{\mathcal{E}}$ in the above denominator, was obtained as the Tamagawa number at 7, which was 3. Now the same method of descent via isogeny as in the previous example allows us to determine the precise order of $\#Ш(\widehat{\mathcal{E}}/\mathbb{Q})[9]$:

$$\begin{aligned}\mathrm{Sel}^{(\widehat{\phi})}(\widehat{\mathcal{E}}/\mathbb{Q}) &= \beta_7^{-1}\Big(F_7\Big(\mathcal{E}(\mathbb{Q}_7)/\widehat{\phi}\big(\widehat{\mathcal{E}}(\mathbb{Q}_7)\big)\Big)\Big)\bigcap\langle 2,3,7\rangle \\ &= \langle 7^3\rangle\{2^{k_2}\cdot 3^{k_3}\cdot 17^{k_{17}} : 0\leqslant k_i\leqslant 8 \text{ and } k_2 + 2\cdot k_3 \equiv 0 \bmod 3\},\end{aligned}$$

so that $\#\mathrm{Sel}^{(\widehat{\phi})}(\widehat{\mathcal{E}}/\mathbb{Q}) = 9^2$. Using the formula from Theorem 3, we see that this implies $\#\mathrm{Sel}^{(\phi)}(\mathcal{E}/\mathbb{Q}) = 1$. Since also $\#\mathcal{E}(\mathbb{Q})[\phi] = 9$, $\#\widehat{\mathcal{E}}(\mathbb{Q})[9] = 1$, the exact sequence (17) from Lemma 2, with $\mathcal{E}, \widehat{\mathcal{E}}$ interchanged, gives that $\#\mathrm{Sel}^{(9)}(\widehat{\mathcal{E}}/\mathbb{Q}) = 9$, and so $\#Ш(\widehat{\mathcal{E}}/\mathbb{Q})[9] \leqslant 9$. From (22) it follows that $\#Ш(\widehat{\mathcal{E}}/\mathbb{Q})[9] = 9$, and that $\widehat{\mathcal{E}}(\mathbb{Q})$ has rank 0. Hence, we may conclude that $Ш(\widehat{\mathcal{E}}/\mathbb{Q})[3^\infty] \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. □

We now illustrate how Proposition 1 can be used, with minimal computation, to prove the existence of nontrivial members of $Ш(\widehat{\mathcal{E}}/\mathbb{Q})[13]$.

Example 3. The elliptic curve

$$\widehat{\mathcal{E}} : y^2 + xy + y = x^3 - x^2 - 911\,138\,880x - 10\,586\,098\,442\,003$$

is such that $\#Ш(\widehat{\mathcal{E}}/\mathbb{Q})[13] \geq 13^2$.

Proof. Consider

$$\mathcal{E} : y^2 + xy + y = x^3 - x^2 - 1\,005\,630x + 571\,521\,997$$

and

$$\widehat{\mathcal{E}} : y^2 + xy + y = x^3 - x^2 - 911\,138\,880x - 10\,586\,098\,442\,003.$$

There exists a $\mathbb{Q}$-rational isogeny of degree 13 such that $\phi : \mathcal{E} \to \widehat{\mathcal{E}}$. Using Magma (2007) to perform a complete 2-descent on $\mathcal{E}$, we see that $\mathrm{rank}(\mathcal{E}(\mathbb{Q})) = \mathrm{rank}(\widehat{\mathcal{E}}(\mathbb{Q})) = 0$. Further, recall that elliptic curves cannot have rational torsion points of order 13. Hence, we have from Proposition 1, with $\mathcal{E}, \widehat{\mathcal{E}}$ interchanged, that

$$\#Ш(\widehat{\mathcal{E}}/\mathbb{Q})[13] \geqslant \left(\frac{\#\widehat{\mathcal{E}}(\mathbb{Q})[\widehat{\phi}]\ \ \Omega_{\mathcal{E}}\ \ \prod_p c_{\mathcal{E},p}}{\#\mathcal{E}(\mathbb{Q})[\phi]\ \ \Omega_{\widehat{\mathcal{E}}}\ \ \prod_p c_{\widehat{\mathcal{E}},p}}\right)\left(\frac{1}{\#\mathcal{E}(\mathbb{Q})[\phi]/\widehat{\phi}(\widehat{\mathcal{E}}(\mathbb{Q})[13])}\right)$$
$$\times \left(\frac{1}{\#\widehat{\mathcal{E}}(\mathbb{Q})/[13]\widehat{\mathcal{E}}(\mathbb{Q})}\right) = \left(\frac{\Omega_{\mathcal{E}}\ \prod_p c_{\mathcal{E},p}}{\Omega_{\widehat{\mathcal{E}}}\ \prod_p c_{\widehat{\mathcal{E}},p}}\right) = \left(\frac{(13\Omega_{\widehat{\mathcal{E}}})\cdot 52}{(\Omega_{\widehat{\mathcal{E}}})\cdot 4}\right) = 13^2.$$

Note that the above global Tamagawa number of 52 for $\mathcal{E}$ in the numerator, was obtained as the product of the Tamagawa numbers at 2, 5, 17, which were 13, 2, 2, respectively. The global Tamagawa number of 4 for $\widehat{\mathcal{E}}$ in the above denominator, was obtained as the product of the Tamagawa numbers at 5, 17, which were 2, 2, respectively. So we have found an elliptic curve with nontrivial 13-part of $Ш(\widehat{\mathcal{E}}/\mathbb{Q})$. However, to find the actual size of $Ш(\widehat{\mathcal{E}}/\mathbb{Q})[13]$, we would need to actually compute $\mathrm{Sel}^{(13)}(\widehat{\mathcal{E}}/\mathbb{Q})$. As a point of interest, note that we can use Magma (2007) to see that the Birch and Swinnerton-Dyer conjecture (see Wiles (2001)) predicts that $\#Ш(\widehat{\mathcal{E}}/\mathbb{Q}) = 13^2$, which coincides with the above lower bound for $\#Ш(\widehat{\mathcal{E}}/\mathbb{Q})[13]$. □

We finally note some possible future generalisations. First, our restriction that d is a prime power was merely for computational convenience, and minor modifications of the above should also deal with elliptic curves with rational points of order $d = 10, 12$, while still working over the ground field. Second, the requirement that the ground field should be $\mathbb{Q}$ was again merely for computational convenience, and in principle could be extended to any number field. Furthermore, as we have already noted in Example 3, there are isogenies of degree d defined over the ground field, even when there does not exist a rational point of order d; when d is a prime power, this makes families of curves available for $d \in \{2, 3, 4, 5, 7, 8, 9, 13, 16, 25\}$, and sporadically occurring curves for $d \in \{11, 17, 19, 27, 37, 43, 67, 163\}$. This gives us a range of curves for

which we can find the rank, with a method other than a complete 2-descent, and a means of finding interesting orders of the Tate–Shafarevich group.

References

Batut, C., Belabas, K., Bernardi, D., Cohen, H., Olivier, M., 2007. PARI Computer Algebra Package. Université Bordeaux I. Available at: http://pari.math.u-bordeaux.fr/.

Beaver, C.D., 2000. 5-torsion in the Shafarevich–Tate group of a family of elliptic curves. J. Number Theory 82, 25–46.

Cassels, J.W.S., 1959. Arithmetic on curves of genus 1. I. On a conjecture of Selmer. J. Reine Angew. Math. 202, 52–99.

Cassels, J.W.S., 1965. Arithmetic on curves of genus 1, VIII. On conjectures of Birch and Swinnerton-Dyer. J. Reine Angew. Math. 217, 180–199.

Cassels, J.W.S., 1995. Lectures on Elliptic Curves. In: London Mathematical Society Student Texts, vol. 24. Cambridge University Press.

Conrad, B., Rubin, K. (Eds.), 2001. Arithmetic Algebraic Geometry. American Mathematical Society.

Cremona, J.E., 2005. mwrank. Available at: http://www.warwick.ac.uk/~masgaj/ftp/progs/mwrank.info.

Cremona, J.E., Fisher, T.A., O'Neil, C., Simon, D., Stoll, M., 2006. Explicit n-descent on elliptic curves: I. Algebra. http://www.arxiv.org/abs/math.NT/0606580.

Cremona, J.E., Serf, P., 1999. Computing the rank of elliptic curves over real quadratic number fields of class number 1. Math. Comput. 68 (227), 1187–1200.

Delong, M., 2002. A formula for the Selmer group of a rational three-isogeny. Acta Arith. 105, 119–131.

Djabri, Z., Schaefer, E.F., Smart, N.P., 2000. Computing the p-Selmer group of an elliptic curve. Trans. Amer. Math. Soc. 352 (1), 5583–5597.

Elkies, N., Rogers, N.F., 2004. Elliptic curves $x^3 + y^3 = k$ of high rank. In: Buell, D. (Ed.), Proceedings of ANTS-VI. In: Lecture Notes in Computer Science, vol. 3076. pp. 184–193.

Fisher, T., 2000. On 5 and 7 descents for elliptic curves. Ph.D. Thesis, Cambridge.

Fisher, T., 2001. Some examples of 5 and 7 descent for elliptic curves over $\mathbb{Q}$. J. European Math. Soc. 3, 169–201.

Flynn, E.V., Grattoni, C., 2007. PARI programs and more detailed descriptions of the algorithms. Made available at: http://www.maths.ox.ac.uk/~flynn/genus2/flynngrattoni/.

Goins, E.H., 2004. Explicit descent via 4-isogeny on an elliptic curve. http://arxiv.org/abs/math.NT/0411215.

Husemöller, D., 2003. Elliptic Curves. Springer.

Kloosterman, R., Schaefer, E., 2003. Selmer groups of elliptic curves that can be arbitrarily large. J. Number Theory 99 (1), 148–163.

Kloosterman, R., 2005. The p-part of the Tate–Shafarevich groups of elliptic curves can be arbitrarily large. J. Théor. Nombres Bordeaux 17 (3), 787–800.

The magma computational algebra system, 2007. Available from: http://magma.maths.usyd.edu.au/magma/.

Matsuno, K., 2007. Construction of elliptic curves with large Iwasawa λ-invariants and large Tate–Shafarevich groups. Manuscripta Math. 122, 289–304.

Mazur, B., 1978. Rational isogenies of prime degree. Invent. Math. 44, 129–162.

Merriman, J.R., Siksek, S., Smart, N., 1996. Explicit 4-descents on an elliptic curve. Acta Arith. 77, 385–404.

Schaefer, E.F., 1996. Class groups and selmer groups. J. Number Theory 56, 79–114.

Schaefer, E.F., 1998. Computing a Selmer group of a Jacobian using functions on the curve. Math. Ann. 310, 447–471.

Schaefer, E.F., Stoll, M., 2004. How to do a p-descent on an elliptic curve. Trans. Amer. Math. Soc. 356, 1209–1231.

Silverman, J.H., 1986. The Arithmetic of Elliptic Curves. Springer.

Stamminger, S., 2005. Explicit 8-descent on elliptic curves. Ph.D. Thesis, International University Bremen.

Tate, J., 1975. Algorithm for determining the type of a singular fiber in an elliptic pencil. In: Modular Functions of One Variable IV. In: Lecture Notes in Mathematics, vol. 476. Springer.

Top, J., 1993. Descent by 3-isogeny and 3-rank of quadratic fields. Adv. Number Theory, 303–317.

Vélu, J., 1971. Isogénies entre courbes elliptiques. C. R. Acad. Sci. Paris, Série A 273, 238–241.

Wiles, A., 2001. The Birch and Swinnerton-Dyer conjecture. Clay Math Institute Problem Description. http://www.claymath.org/millennium/Birch_and_Swinnerton-Dyer_Conjecture/BSD.pdf.

Womack, T., 2000. A Mestre-style search for high-rank curves of small conductor. http://www.tom.womack.net/maths/mestre.gp.